PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039082
(43)Date of publication of application : 12.02.1999

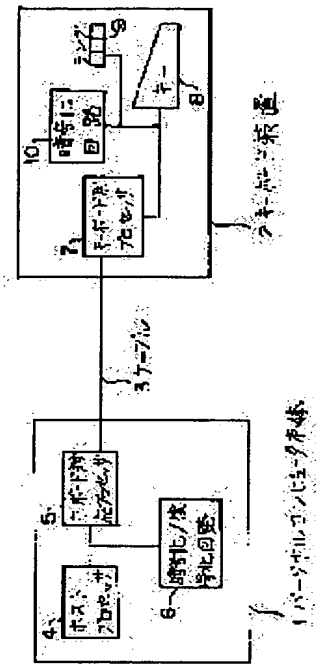
(51)Int.Cl. G06F 3/02
G06F 1/00
H04L 9/08
H04L 9/10
H04L 9/32
H04L 9/36

(21)Application number : 09-190065
(22)Date of filing : 15.07.1997

(71)Applicant : FUJITSU LTD
(72)Inventor : HIGUCHI TAIHO

(54) KEYBOARD DEVICE HAVING SECURITY FUNCTION AND METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a keyboard device having a high security function.
SOLUTION: A ciphering/decoding circuit 6 and a ciphering circuit 10 are provided for a main body 1 and the keyboard device 2. The keyboard device 2 waits for the input of user ID and a password from a key 8 with the power supply of the main body 1. When a user ID is inputted and it is transmitted to the main body 1, random numbers for message-compressing the password are transmitted from the main body 1 to the keyboard device 2. The keyboard device 2 message-compresses the password by the random numbers and transmits it to the main body 1. The main body 1 compares the password which is transmitted and message-compressed with the password which is message-compressed inside and certifies a user. An open key is transferred to the keyboard device 2 and a cipher key used for session is transmitted from the keyboard device 2 to the main body 1. Then, session is executed by using the open key hereafter.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－39082

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	3/02	３８０	Ｇ０６Ｆ	3/02	３８０Ｂ
	1/00	３７０		1/00	３７０Ｅ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
	9/10				６０１Ｅ
	9/32				６２１Ａ

審査請求　未請求　請求項の数16　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平9－190065

(22)出願日　平成９年(1997)７月15日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　樋口　大奉
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　弁理士　大菅　義之　（外１名）

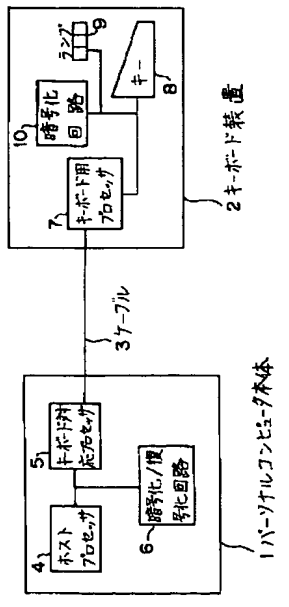
(54)【発明の名称】　機密保持機能を有するキーボード装置及びその方法

(57)【要約】

【課題】機密保持機能の高いキーボード装置を提供することである。

【解決手段】本体１とキーボード装置２に暗号化／復号化回路６及び暗号化回路１０を設ける。本体１の電源投入によりキーボード装置２は、キー８からのユーザＩＤ及びパスワードの入力待ちとなる。ユーザＩＤが入力され、本体１へ送信されると、今度は本体１からパスワードをメッセージ圧縮するための乱数がキーボード装置２に送られ、キーボード装置２はパスワードを乱数によってメッセージ圧縮して本体１へ送信する。本体１では、送信されてきたメッセージ圧縮されたパスワードと内部でメッセージ圧縮したパスワードとを比較し、利用者の認証を行う。次に、キーボード装置２に公開鍵が渡され、キーボード装置２からセッションに使う暗号鍵が本体１に送信される。そして、以後、この暗号鍵を用いてセッションを行う。

本発明のキーボード装置の第1の実施形態の構成を示す図



【特許請求の範囲】

【請求項１】コンピュータ装置の本体に接続されて用いられるキーボード装置であって、
前記本体に送出する信号を暗号化する暗号化手段と、
暗号化された前記信号を送出する送出手段とを備えることを特徴とするキーボード装置。

【請求項２】前記本体の電源投入後に、前記本体に対して利用者のパスワードを暗号化して送信することを特徴とする請求項１に記載のキーボード装置。

【請求項３】前記パスワードを入力した前記利用者が前記本体において正当な利用資格者と認証された場合に、前記本体へ送信する信号の送信を暗号化して行うための暗号鍵を前記本体に送信することを特徴とする請求項２に記載のキーボード装置。

【請求項４】前記暗号鍵は前記本体から送信されてきた公開鍵に基づいて暗号化して前記本体に送信することを特徴とする請求項３に記載のキーボード装置。

【請求項５】前記キーボード装置に何の入力も無い場合にも、ダミーデータを暗号化して、前記本体に対して定常的に送出することを特徴とする請求項１に記載のキーボード装置。

【請求項６】前記本体に送出する信号の少なくとも一部を光信号に変換して、前記本体に送出することを特徴とする請求項１に記載のキーボード装置。

【請求項７】前記キーボード装置の操作者が所定の時間入力を行わないことにより前記信号を暗号化することを中止することを特徴とする請求項１に記載のキーボード装置。

【請求項８】前記キーボード装置に設けられるキーボード用プロセッサと前記暗号化手段とを一体化して、容易に分解できないように封入したことを特徴とする請求項１に記載のキーボード装置。

【請求項９】前記本体側よりの指示により、前記信号を暗号化しない通常の動作モードと、前記信号を暗号化する暗号化モードの切り換え可能に構成され、暗号化モードに入ったことを示す特有の表示を行うことを特徴とする請求項１に記載のキーボード装置。

【請求項１０】コンピュータ装置の本体に接続されて用いられるキーボード装置と前記本体との間の通信の機密を保持する方法であって、
前記本体に送出する信号を暗号化するステップと、
暗号化された前記信号を送出するステップとを備えることを特徴とするコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１１】前記本体の電源投入後に、前記本体に対して前記コンピュータ装置の利用者のパスワードを暗号化して送信することを特徴とする請求項１０に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１２】前記パスワードを入力した前記利用者が

前記本体おいて正当な利用資格者と認証された場合に、前記本体へ送信する信号の送信を暗号化して行うための暗号鍵を前記本体に送信することを特徴とする請求項１１に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１３】前記暗号鍵は前記本体から送信されてきた公開鍵に基づいて暗号化して前記本体に送信することを特徴とする請求項１２に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１４】前記キーボード装置に何の入力も無い場合にも、ダミーデータを暗号化して、前記本体に対して定常的に送出することを特徴とする請求項１０に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１５】前記本体に送出する信号の少なくとも一部を光信号に変換して、前記本体に送出することを特徴とする請求項１０に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【請求項１６】前記キーボード装置の操作者が所定の時間入力を行わないことにより前記信号を暗号化することを中止することを特徴とする請求項１０に記載のコンピュータ本体とキーボード装置との間の通信の機密保持方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、機密保持機能を有するキーボード装置、及びコンピュータ本体とキーボード装置間の通信の機密保持方法に関する。

【０００２】

【従来の技術】コンピュータによる犯罪の可能性が指摘されてから、データの保全と利用者の特定のために多くの保護手段が用いられるようになった。これには暗号化やパスワードによる利用者の特定などがある。

【０００３】しかし、その反面で最もポピュラーな入力手段であるキーボード装置については安全性が極めて低いのが現状である。特に、デスクトップタイプの分離型のキーボード装置は標準化が行われ、低コストである反面で安全性についてはほとんど考慮されていない。長いケーブルで比較的に高いレベルの信号を扱っていることで、ここを流れる信号は容易に外部で拾い出して復元することができる。またキーボード本体も容易に分解可能な構造であり、操作性からある程度の大きさを必要としながら軽量化されているために内部は空洞状態で盗聴器（キーボード装置のキーから入力される信号を外部から取得する装置を盗聴器と読んでおり、以降、このような外部からの信号の取得を盗聴という）を配置することも容易である。

【０００４】図７は、従来のキーボード装置及びパーソナルコンピュータ本体の構成の一例を示す図である。７１は、パーソナルコンピュータ本体であり、表示装置等

は図示されていないが通常のパーソナルコンピュータが備える表示装置等は備えているものとする。７２はキーボード装置である。７３は両者を接続するケーブルである。パーソナルコンピュータ本体７１にはキーボード装置７２からの信号を受け取るキーボード対応プロセッサ７５があり、ここでキーボード装置７２のキー７７を押すことによって生成される符号（文字コード等）の変換とホストプロセッサ７４へキーボード装置７２から入力されたデータを送信するための割り込み等を行う。キーボード装置７２にもキーボード用プロセッサ７６が格納され、キーボード用プロセッサ７６はキーボード装置７２のキー７７のどのキーが打鍵されたかを判断して、対応する符号の生成を行う。ケーブル７３は、上りまたは下り（キーボード装置７２からパーソナルコンピュータ本体７１へ向かう方向を上りとしている）の信号を送出する信号線、クロック線、電源線等からなり、パーソナルコンピュータ本体７１からのコマンド、キーボード装置７２からの信号がシリアルに伝送される。キーボード装置７２にはキー７７及び大文字／数字などのモードを表示する、パーソナルコンピュータ本体７１の制御により点灯／滅灯されるランプ７８がある。キー７７が打鍵されることによりその位置と同時に打鍵の情報がキーボード用プロセッサ７６によって変換されてケーブル７３を通してパーソナルコンピュータ本体７１に送出される。

【０００５】

【発明が解決しようとする課題】従来、無資格者による操作の防止のために、キーボード装置をパスワードでロックすることは実施されてきた。これは、パーソナルコンピュータ本体側のキーボード装置からの符号（コード）を解読する専用プロセッサ（図７のキーボード対応プロセッサ７５）内に所定の文字列を予め設定しておき、キーボード装置からこれに一致する文字列が入力されるまで、全ての入力を無視することにより無資格者の操作が行えないようにする方法である。

【０００６】しかし、この場合にもパスワードなどの入力はキーボードから行われるので、このパスワードを表す信号が外部で収集可能であれば折角の保護手段も効果がなくなってしまう。

【０００７】従って、ホテルや公共の場に配置されるパーソナルコンピュータが操作する資格の無い人に操作されたり、パスワードが盗まれたりする可能性がある。本発明の課題は、機密保持機能の高いキーボード装置を提供することである。

【０００８】

【課題を解決するための手段】本発明によるキーボード装置は、コンピュータ装置の本体に接続されて用いられるキーボード装置であって、前記本体に送出する信号を暗号化する暗号化手段と、暗号化された前記信号を送出する送出手段とを備えることを特徴とする。

【０００９】また、本発明による機密保持方法は、コンピュータ装置の本体に接続されて用いられるキーボード装置と前記本体との間の通信の機密を保持する方法であって、前記本体に送出する信号を暗号化するステップと、暗号化された前記信号を送出するステップとを備えることを特徴とする。

【００１０】上記本発明の構成によれば、コンピュータ装置の本体へキーボード装置から情報を送る場合に、暗号化して送るので、コンピュータ装置とキーボード装置とを接続するケーブルの部分で盗聴されても容易には情報を盗まれることがない。

【００１１】また、コンピュータ装置が起動した状態で、すぐに、利用者にユーザＩＤとパスワードの入力を行うが、このパスワードも暗号化あるいはメッセージ圧縮してコンピュータ装置本体に送信するようにすることによって、パスワードそのものが盗聴されることを防ぐことができる。

【００１２】このように、キーボード装置からコンピュータ装置本体に情報が送信される間のケーブルの部分での盗聴を困難にすることが出来るので、機密保持機能の高いキーボード装置を提供することができる。

【００１３】

【発明の実施の形態】図１は、本発明のキーボード装置の第１の実施形態の構成を示す図である。パーソナルコンピュータ本体１にはホストプロセッサ４及びキーボード対応プロセッサ５が従来の構成と同様に設けられているが、本実施形態においては、更に、暗号化／復号化回路６が設けられている。また、キーボード装置２は、従来の構成であるキーボード用プロセッサ７、キー８、及びランプ９を備えると共に、暗号化回路１０を備えている。パーソナルコンピュータ本体１に設けられる暗号化／復号化回路６及びキーボード装置２に設けられる暗号化回路１０は、パーソナルコンピュータ本体１とキーボード装置２との間でケーブル３を介して転送されるデータあるいは符号（文字コード）等を暗号化するためのものである。パーソナルコンピュータ本体１とキーボード装置２との間を転送される符号等を暗号化することにより、ケーブル３のどこかに盗聴装置が取り付けられていても、盗聴した者は、ケーブル３を転送されている符号がどのようなものか解読することが容易でないので、機密保持機能を高めることが出来る。

【００１４】なお、パーソナルコンピュータ本体１のホストプロセッサ４は、パーソナルコンピュータの一般的な処理を行うプロセッサであり、アプリケーションの実行などを行う。キーボード対応プロセッサ５は、キーボード装置２から送られてくる符号を表す信号を意味のある文字コード等に変換してホストプロセッサ４に渡す役割をしており、ホストプロセッサ４とキーボード装置２とのインターフェースを行うものである。キーボード装置２のキーボード用プロセッサ７は、キー８で生成され

た信号を、パーソナルコンピュータ本体１のキーボード対応プロセッサ５が意味のある文字コード等に変換できるような符号に変換するインタフェースの役割を行うものである。ランプ９は、キー８の特殊キーを押下することによって入力モード等がどういう状態にあるかを示すもので、パーソナルコンピュータ本体１からの指示によりキーボード用プロセッサ７が制御するものである。例えば、ランプ９は大文字入力の場合に点灯させる。

【００１５】本実施形態では、パスワードをキーボード装置２からパーソナルコンピュータ本体１に送信する場合にも、乱数を用いてパスワードをメッセージ圧縮して送信するようにするので、ケーブル３の途中で盗聴されても盗聴した者にはパスワードが分からないようになっている。この乱数はパーソナルコンピュータ本体１からキーボード装置２に送信され来たものを使う。この場合にも、キーボード装置２は、パスワードを乱数でメッセージ圧縮して送信し、パーソナルコンピュータ本体２は送信されてきたメッセージ圧縮されたパスワードと内部で圧縮したパスワードとを圧縮されたままの状態で比較する。

【００１６】パスワードをキーボード装置２から入力すると、パーソナルコンピュータ本体１は以後にケーブル３を用いて転送される符号の暗号化のための鍵をキーボード装置２へ送信する。この暗号鍵を盗聴されては、機密保持機能が保てないので、暗号鍵も暗号化して送信するようにする。この暗号鍵を暗号化するための鍵は公開鍵を使用するようにする。すなわち、パーソナルコンピュータ本体１からキーボード装置２へ公開鍵を予め送信する様にする。公開鍵は第３者が取得しても、事実上、その公開鍵で暗号化されたデータを解読することは不可能なので、ケーブル３の途中で盗聴されても問題は生じない。

【００１７】公開鍵を使用して符号の暗号化に必要な暗号鍵をパーソナルコンピュータ本体１からキーボード装置２へ送信し、その後は、公開鍵を使って暗号化されて送信された暗号鍵に基づいて処理速度の速い暗号化方法を使って符号の転送を行う。暗号鍵が暗号化されて送信されるので、盗聴されても第３者にはパーソナルコンピュータ本体１とキーボード装置２との間の符号の転送の内容を知られることはない。

【００１８】電源投入時のような場合、キーボード装置２はパスワードの投入待ち状態となる。これはパーソナルコンピュータ本体１からの指示により例えばランプ９を複数個同時に点滅させる等の手段で示される。ここで操作者が改行キーで終わる一連のパスワードを入力すると、パーソナルコンピュータ本体１より送信された乱数とこのパスワードを組み合わせて、例えば、ＭＤ５に基づくメッセージ圧縮を行い、その結果がパーソナルコンピュータ本体１に送出される。パーソナルコンピュータ本体１ではこの結果を内部の同様にして圧縮されたパスワードと照合することで操作者が利用資格者であることを認識できる。次に、パーソナルコンピュータ本体１は固有の公開鍵をキーボード装置２に送出する。キーボード装置２はこの公開鍵により、このセッションに使用する暗号鍵をパーソナルコンピュータ本体１に送出し、これ以降はキーボード装置２からの送出データは全て暗号化してパーソナルコンピュータ本体１に送出する。この暗号化は利用者からのリセット指示、パーソナルコンピュータ本体１からのセッションの終了または一定時間入力がない等による切断により解除され、キーボード装置２は再びパスワードの入力待ちになる。これらの暗号化の解除はホストプロセッサ４の監視の下に行われる。

【００１９】ＭＤ５はメッセージを所定のルールに従い圧縮する算法である。この圧縮結果を同じ圧縮方法で圧縮されたメッセージと比較することで元のメッセージとの同一性が高い確率で保障される。逆に圧縮前のデータの一部と圧縮結果から元のメッセージを復元することは困難である。このことから安全でない伝送手段を用いての認証の手段として用いられるものである。ＭＤ５の詳細については、インターネット・アーキテクチャ委員会が発行する標準勧告文書である以下の文書を参照されたい。「Network Working Group, Request for Comments: 1321, The MD5Message-Digest Algorithm, R.Rivest, MIT Laboratory for Computer Scienceand RSA Data Security, Inc., April 1992」

公開暗号鍵は、ここではＲＳＡ方式等の公開鍵を使用する。元来が一定期間の保護で十分なパスワード等の保護が目的であるから、暗号の強度すなわち鍵の長さはコスト・性能のトレードオフにより決定される。本実施形態では、パーソナルコンピュータ本体１側が秘密鍵を持ち、キーボード装置２に対して公開鍵を送出する。公開鍵であるので仮に傍受されても問題は発生しない。キーボード装置２のコストを下げるために、例えば、秘密鍵とモジュロ数は５１２ビット相当、公開鍵は３２ビット相当などの値が選ぶのが好ましい。

【００２０】図２は、本実施形態のキーボード装置の構成の一例を示す図である。図１にも示したように、キーボード装置はキー８、キーボードＣＰＵ（キーボード用プロセッサ）７、及び暗号化回路１０からなる。キー８には、「ａ」、「ｂ」、「ｃ」等の各記号を表すキーが複数配列されており、各キーにはそのキーが存在する位置をＸ座標とＹ座標で表すための配線２０、２１がなされている。キー８のいずれか１つのキーが押されると、この配線２０、２１に信号が流れ、キーボードＣＰＵ７に、押下されたキーのＸ座標位置とＹ座標位置を入力するようになっている。

【００２１】キーボードＣＰＵ７は、このＸ座標位置とＹ座標位置の入力を受けて、押下されたキーに対応する記号が何かを演算し、パーソナルコンピュータ本体１に送信するための符号を生成する。更に、本実施形態で

は、キーボードＣＰＵ７が生成した符号を暗号化回路１０で暗号化して、キーボードＣＰＵ７に返して、ケーブル３を介してパーソナルコンピュータ本体１に送出する。

【００２２】暗号化回路１０がキーボードＣＰＵ７で生成された符号を暗号化する場合に、使用する暗号鍵は、前述したように、公開鍵を用いてパーソナルコンピュータ本体１に送信された暗号鍵であり、暗号化回路１０に組み込まれているものである。前述したように、キーボード装置２は、標準化および軽量化が図られていて、安価であるが、簡単に分解可能な構成となっている。したがって、暗号化回路１０が符号の暗号化に使う暗号鍵を盗もうとすれば、キーボード装置２を分解して、中にある暗号化回路１０を解析すれば、暗号鍵を盗むことが出来る。このように、キーボード装置２内に暗号化回路１０を設けただけでは、機密保持機能は万全ではない。

【００２３】そこで、本実施形態では、キーボードＣＰＵ７と暗号化回路１０とを樹脂などで固めるなどして、パッケージ化する。このようにすれば、暗号化回路１０を容易には取り外すことができなくなると共に、暗号化回路１０を調べることが難しくなるので暗号化回路１０から暗号鍵が盗まれる可能性を小さくすることができる。

【００２４】すなわち、従来用いられているキーボードのＸ、Ｙ座標の位置情報をキーボードＣＰＵ７がどう利用しているかは外部からは観測されないので、この限りでは安全である。しかし、本実施形態によるキーボードＣＰＵ７と暗号化回路１０の間の配線はキー８の押下に対応する符号などクリティカルな信号が流されるので外部に漏洩しない措置が必要である。そこで、例えば、両者を一個のパッケージに封入したり、金属箔で覆って樹脂等で容易に剥がれないようにするのである。

【００２５】図３は、本実施形態の一連の処理フローを表すタイムチャートである。先ず、電源が入れられシステムが立ち上がると、パーソナルコンピュータ本体１からキーボード装置２へ、暗号モード移行指示が出される。暗号モードとは、パーソナルコンピュータ本体１とキーボード装置２との間のデータの転送を暗号化して行う動作モードのことである。キーボード装置２側で暗号モードを使用する旨の応答をすると、キーボード装置２はユーザＩＤとパスワードの入力待ちとなる。ここで、図３には示されていないが、キーボード装置２で暗号モードを使用しない旨の応答を行った場合には、以下の処理は行われず、キーボード装置２からの符号等の転送は暗号化を行わない通常の処理となる。

【００２６】まず、キーボード装置２からユーザＩＤが入力されたら、このユーザＩＤは暗号化せずに直接パーソナルコンピュータ本体１に送信される。パーソナルコンピュータ本体１では、これにより、ユーザ登録の確認が行われる。次に、キーボード装置２の使用者を認証するために、パーソナルコンピュータ本体１側から乱数をキーボード装置２に送出する。キーボード装置２ではユーザの入力したパスワードとパーソナルコンピュータ本体１から送信されてきた乱数から所定の算法（例えば、ＭＤ５）により圧縮したメッセージをパーソナルコンピュータ本体１に送出する。パーソナルコンピュータ本体１側では、キーボード装置２から送信されてきたメッセージ圧縮されたパスワードと、パーソナルコンピュータ本体１内部に記録されているパスワードを同じ乱数を用いて同じ方法（ここでは、ＭＤ５）で圧縮したパスワードとを圧縮されたままの形で比較し、一致するか否かを判断する。一致した場合には、このパスワードを入力した利用者が正当な使用者であることが認められたことになる。

【００２７】パーソナルコンピュータ本体１側で利用者が正当なものと確認できると、両者間での暗号の設定を行う。この場合、パーソナルコンピュータ本体１からキーボード装置２に送られるデータとキーボード装置２からパーソナルコンピュータ本体１に送られるデータの両方を暗号化することが考えられる。しかし、実際には、キーボード装置２からパーソナルコンピュータ本体１に送出されるデータが保護されれば十分であるので以下のような処理とする。

【００２８】先ず、パーソナルコンピュータ本体１から公開鍵とモジュロの除数をキーボード装置２に送出する。キーボード装置２はこの公開鍵とモジュロの除数より、暗号モードでの符号送信に使用するＤＥＳ暗号鍵をパーソナルコンピュータ本体１に送出する。パーソナルコンピュータ本体１では、暗号化されたＤＥＳ鍵を復号する。そして、以後、キーボード装置２から送出されるデータは、このＤＥＳ鍵により暗号化されたデータを使用する。キーボード装置２は、パーソナルコンピュータ本体１に送信するデータをＤＥＳ鍵で暗号化しながら送信し、パーソナルコンピュータ本体１は、送信されてくる暗号化されたデータをＤＥＳ鍵で復号しながらパーソナルコンピュータ本体１のホストプロセッサ４に供給する。

【００２９】なお、上記一連の処理は、パーソナルコンピュータ本体１のキーボード対応プロセッサ５、暗号化／復号化回路６、及びキーボード装置２のキーボード用プロセッサ７、暗号化回路１０によって行われる。

【００３０】図４は、キーボード装置側の一連の処理を示した図である。先ず、パーソナルコンピュータ本体１で電源が入れられると、パーソナルコンピュータ本体１にケーブル３で接続されたキーボード装置２にも電源が投入される（ステップＳ１）。電源が投入されると、キーボード装置２のキーボード用プロセッサ７はキー８から暗号モードを設定する指示が来ているか否かの判断を行う（ステップＳ２）。キー８から暗号モードを設定する指示がない場合には、ステップＳ１２に進み、通常モ

ードによって、キーボード装置２から入力されるデータを暗号化せずにパーソナルコンピュータ本体１に送出する。

【００３１】ステップＳ２で、キー８から暗号モードを設定する指示があった場合には、キーボード用プロセッサ７がキーボード装置２をユーザＩＤ及びパスワードの入力待ち状態にする。このとき、ユーザＩＤ及びパスワードの入力待ち状態をランプ９を点滅することによって表示する。

【００３２】なお、パスワードを盗む方法として、アプリケーションプログラムのレベルで、あたかも初期パスワードの入力モードであるかのように、ユーザに錯誤を起こさせる手法が用いられることがある。これを防止するためには画面上の指示と同時にキーボード装置２側の表示も同時に行い、しかもこの状態がアプリケーションでは容易に実現できないようにすることが有効である。通常キーボード装置２には次の３個の表示ランプ９がついている。「大文字入力モード表示」、「スクロールしないモード表示」、「数字入力表示」である。これらのランプ９は、パーソナルコンピュータ本体１側からの指示を受けてキーボード装置２内のキーボード用プロセッサ７が点灯、滅灯を行う。これを通常とは明らかに違う（例えば、特定の周期で全灯が点滅を行う）状態にすることで、パスワードの投入が必要な状態にあることを知らせる（このとき、パーソナルコンピュータ本体１の表示画面には、パスワードの投入が必要な状態にある旨の指示が表示される）。

【００３３】この特定の点滅指示が暗号化モード以外の場合に発生しないようにするには、キーボード装置２側で各ランプ９のランプ点滅指示があった場合には同時でなく、僅かな時間（０．５秒ほど）すらして実行するようにし、動作モード切り換えのコマンドに対してのみ完全に同時に点滅するようにすることで実現できる。

【００３４】ステップＳ３でユーザＩＤ及びパスワード入力待ち状態に入ると、ユーザからユーザＩＤが入力されるのを待つ。ユーザＩＤが入力されると、ステップＳ４でユーザＩＤをキーボード装置２からパーソナルコンピュータ本体１へ送信する。パーソナルコンピュータ本体１にユーザＩＤを送信すると、次に、乱数がパーソナルコンピュータ本体１から送信されてくるので、ステップＳ５で乱数を受信する。

【００３５】すると、次に、パスワード入力待ちとなり、ユーザからのパスワードの入力を待つ。ユーザからパスワードが入力されると、キーボード装置２のキーボード用プロセッサ７は、この送信されてきた乱数を用いてパスワードをＭＤ５でメッセージ圧縮し、パーソナルコンピュータ本体１に送信する（ステップＳ６）。パーソナルコンピュータ本体１側では、メッセージ圧縮されたパスワードを受け取ると、自身内部に保持しているパスワードを同じ乱数を使ってＭＤ５でメッセージ圧縮したものと比較し、一致するか否かの判定結果をキーボード装置２に送信する。

【００３６】キーボード装置２側では、パーソナルコンピュータ本体１からユーザＩＤとパスワードの一致が確認された旨の通知が来たかいなかが判断され（ステップＳ７）、一致していない旨の通知を受け取った場合には、ステップＳ３に戻って、再びユーザからのユーザＩＤとパスワードの入力待ちとなる。このとき、パーソナルコンピュータ本体１の表示には、入力されたユーザＩＤとパスワードではユーザの認証が行えなかった旨の表示を行うようにする。

【００３７】ステップＳ７で、パーソナルコンピュータ本体１からユーザの認証が成功した旨の通知を受けた場合には、次にパーソナルコンピュータ本体１からＤＥＳの暗号鍵をキーボード装置２から送信するための公開鍵が暗号化／復号化回路６で生成されて送られてくるので、これを受信する（ステップＳ８）。キーボード装置７では、暗号化回路１０がこの公開鍵を使って、後のセッション（キーボード装置２からパーソナルコンピュータ本体１へ暗号化した符号を送信する一連の処理）に使われる暗号鍵を暗号化し、キーボード用プロセッサ７を介してパーソナルコンピュータ本体１へ送信する。

【００３８】キーボード装置２では、キーボード用プロセッサ７が乱数を発生し、これによりＤＥＳの暗号鍵を作成し、パーソナルコンピュータ本体１から送信されてきた公開鍵で暗号化してパーソナルコンピュータ本体１に送信する。パーソナルコンピュータ本体１では、このＤＥＳの暗号鍵を復号して暗号化／復号化回路６に設定する。以上により、パーソナルコンピュータ本体１の暗号化／復号化回路６とキーボード装置２の暗号化回路１０には、ＤＥＳの暗号化鍵が設定されるので、以降のデータは、このＤＥＳの暗号鍵を使ってパーソナルコンピュータ本体１にキーボード装置２から暗号化されたデータが送信される（ステップＳ１０）。

【００３９】ユーザＩＤとパスワードを用いたパーソナルコンピュータ本体１への入力セッションが終了した場合には、キーボード装置２から何らかの符号を送信するようにする。ステップＳ１１では、セッションを終了する旨の指示がキーボード装置２から入力された場合に、ステップＳ３に戻って次のセッションを行うため、再び、ユーザＩＤとパスワードの入力待ちとなる。ステップＳ１１でセッションの終了が指示されない場合には、ステップＳ１０とステップＳ１１の処理を繰り返して、暗号化されたキー入力をパーソナルコンピュータ本体１に送信する処理を繰り返す。

【００４０】本実施形態においては、キーボード装置２からパーソナルコンピュータ本体１にパスワードを送る場合、パーソナルコンピュータ本体１側からの乱数を用いて暗号化を行っている。一般に、暗号化に際して暗号・復号鍵が必要になるが、この鍵の配送を更に保護する

ことが必然的に発生する。従って、この乱数の鍵を予めパーソナルコンピュータ本体１とキーボード装置２の間で取り決めてキーボード内のＲＯＭ等に配置することにより実現することが考えられるが、これでは、キーボードは特注品になり、コストもかかる上にキーボードの管理などのコストもかかり、広く一般に利用することは困難となる。

【００４１】従って、本実施形態では、この問題をメッセージ圧縮技術を用いることで解決する。これは同じく乱数を用いるが、この乱数をもとにしてパスワード等の文を一定ルールで変換する方式である。この結果は１：Ｎの対応となり（原文に対し、圧縮された変換文を復元した際の復元データの候補がＮ個対応することになり）、乱数と変換文との両者を入手しても原文（ここではパスワード）を推定することが困難なことを利用する。本体側では正解（パスワード）を知っているので自分で作成したメッセージ圧縮の結果と送られてきたものが、一致すればそのパスワードを入力したユーザを資格者と推定出来るが、これを盗聴している人にはパーソナルコンピュータ本体１及びキーボード装置２の両者の送信するデータを相当量入手しない限り、パスワードの入手が困難である。当然ながら十分なデータが入手出来れば計算等により解読は可能なので、一定期間毎にパスワードを変更することは利用者の責任で行わなければならない。

【００４２】これと、パーソナルコンピュータ本体１とキーボード装置２との間での公開鍵によるデータの暗号化を併用することで、本実施形態においては完全に汎用性のある（量産可能で、どのシステムにも利用可能な）安全なキーボード装置の提供を可能としている。

【００４３】なお、保護を完全なものとするために、データは例えば５６ビットのパケットで送出し、その中の有意なデータの位置はオフセット値を先行データに入れるなどの方法により判定が困難にすることが有効である。キーボード装置２は、パーソナルコンピュータ本体１から送信されてくる公開鍵を用いてＤＥＳの鍵をホストコンピュータに送出する。この際に例えば、キーボードの入れ換えなどの不正が行われないようにするために送出データに加えて、再度先のパスワードを用いた圧縮メッセージを付加して送出することが望ましい。

【００４４】図５は、本実施形態でキーボード装置からパーソナルコンピュータ本体に送信されるデータの構成を説明する図である。キーボード装置２からは有意な情報はキー８を押下したり、離したりしたときにのみ生じる。しかし、このままではキー操作の情報（例えば、入力文字列の長さ等）が容易に漏洩してしまう。これを防止するために、有意なデータがある場合にも無い場合にも同様にキーボード装置２からの信号を送出する。すなわち、キー８が押下されたり、離すことによって生じる有意な情報以外に、ダミー情報を生成してパーソナルコンピュータ本体１に送出するようにする。

【００４５】図５（ａ）は、暗号化された５６ビットのデータがキーボード装置２からパーソナルコンピュータ本体１に対して送出されている様子を模式的に描いた図である。

【００４６】このように、キーボード装置２からはキー８の押下等の有意なデータの生成とは関係なく、所定の間隔で暗号化されたデータをパーソナルコンピュータ本体１に送出する様にする。各暗号化データは内部に有意なデータを持っているか否かの情報を備えるように構成し、パーソナルコンピュータ本体１側でデータを復元した際に、この情報から送信されてきたデータ内に有意なデータが含まれているか否かを判断できるようにする。そして、有意なデータが含まれている場合のみに所定の位置に含まれている有意なデータを取得して、キーボード装置２からパーソナルコンピュータ本体１への入力データとして取り込む。

【００４７】図５（ｂ）は、図５（ａ）の５６ビットの各暗号化データの暗号化前あるいは復号化後のデータの構成を示す図である。暗号化前のデータには、キー８の押下に伴う有意なデータあるいは、キー８の押下等の操作が全く無い状態で生成された無意のデータが９ビット長で含まれている。この９ビットのデータの前には、この９ビットのデータが有意なものか否かを示す１ビットのフラグが設けられる。例えば、この１ビットのフラグが“１”である場合には、次に続くデータは有意なものであることを示し、このフラグが“０”である場合には、次に続くデータは有意なものではないことを示すようにする。従って、５６ビットの暗号化データを復号したパーソナルコンピュータ本体１では、このフラグを見て、“１”であれば次のデータは有意であるのでデータを取り込み、フラグが“０”であれば次のデータは有意ではないので取り込まないという処理を行うようにする。

【００４８】また、図５（ｂ）の暗号化前あるいは復号化後のデータの例では、ダミービットを前後に付加している。これにより、盗聴した者は、たとえ暗号化データを復元することが出来たとしても、どこに意味のあるデータが配置されているのかが分からない。このような構成のデータでは有意のデータを認識可能であるべきパーソナルコンピュータ本体１側でも、どこに有意なデータが含まれているのかが分からなくなってしまう。そこで、次に送信されてくるブロックの９ビットのデータが復号化後のデータの中でどの位置から開始するかを示すデータを９ビットのデータの後ろの位置に配置するようにする。これにより、次に送信されてくる暗号化データのブロックを復号した場合に、フラグ等の意味のあるデータが配置されている場所を見出すことができるので、暗号化データのブロックを生成する際、フラグ等のデータの存在位置を変えることが出来る。これにより、盗聴

されても、盗聴した者は９ビットのデータがどこにあるのかが容易には分からないので、より機密保持機能を向上することができる。

【００４９】このように、暗号モードでの送信中は上りデータはキーボード用プロセッサ７からの送出位置で乱数などの追加を行い、キーの押下の有無にかかわらず定常的に何らかのデータを流し続けることで、入力内容の推定を困難にすることができる。こうして生成されたデータをキーボード装置２の暗号化回路１０でＤＥＳにより暗号化してパーソナルコンピュータ本体１に送信する。

【００５０】図６は、本発明のキーボード装置の第２の実施形態の構成図である。図６において、図１と同じ構成は同じ参照番号が付されており、説明を省略する。本実施形態においては、キー８からの入力を暗号化回路１０で暗号化するとともに、光送受信機６４によって光信号に変換して、パーソナルコンピュータ本体６１に送信する。パーソナルコンピュータ本体６１にも光送受信機６３が設けられており、キーボード装置２からの信号を受け取るとともに、パーソナルコンピュータ本体６１からキーボード装置６２へのデータの転送も光信号を使うことによって行う。これらの光信号は光ケーブル６５によって転送される。

【００５１】本実施形態においては、光ケーブル６５の他に電気的な信号をケーブル６６によって授受するように構成されている。ケーブル６６はパスワード等盗聴されては困るデータ以外のデータ、例えば、ランプ９を点灯させるためのデータや、クロック、電源等をキーボード装置６２に供給するために設けられている。光ケーブル６５とケーブル６６は、別々に設けて、それぞれをパーソナルコンピュータ本体６１に接続するように構成してもよいが、１本のケーブルにまとめて、光接続と電気接続とを１つのコネクタで行えるようにするのが好ましい。

【００５２】光信号は電気信号と異なり、ケーブルを伝搬するとき周囲に誘導電磁場を作らないので、電気信号のように容易に盗聴されることがない。従って、第１の実施形態で述べたような暗号化処理と共に、光信号を使ってパーソナルコンピュータ本体６１とキーボード装置６２の間でパスワードやキー８の押下に対応する符号を送信することにより、盗聴される可能性をかなり小さくすることができる。

【００５３】このように、ユーザＩＤ、パスワード、キー８による入力符号を暗号化すると共に、光信号として授受するようにすることにより、盗聴を防ぐことが出来、更に、機密保持機能の高いキーボード装置を提供することができる。

【００５４】なお、上記実施形態の説明では、コンピュータの本体はパーソナルコンピュータであることを前提に説明したが、本発明はこれに限られるものではなく、コンピュータ本体とキーボード装置とが分離されており、ケーブルで接続されるような構造を有するコンピュータシステムであれば、どのような構成にも適用することができる。

【００５５】

【発明の効果】本発明によれば、例えば、ホテルや公共の場所に設置されたパーソナルコンピュータに外部からのアクセスによる入力データの盗聴や改ざんを困難に出来、安全な運用が可能になる。

【図面の簡単な説明】

【図１】本発明のキーボード装置の第１の実施形態の構成を示す図である。

【図２】本実施形態のキーボード装置の構成の一例を示す図である。

【図３】本実施形態の一連の処理フローを表すタイムチャートである。

【図４】キーボード装置側の一連の処理を示した図である。

【図５】本実施形態でキーボード装置からパーソナルコンピュータ本体に送信されるデータの構成を説明する図である。

【図６】本発明のキーボード装置の第２の実施形態の構成図である。

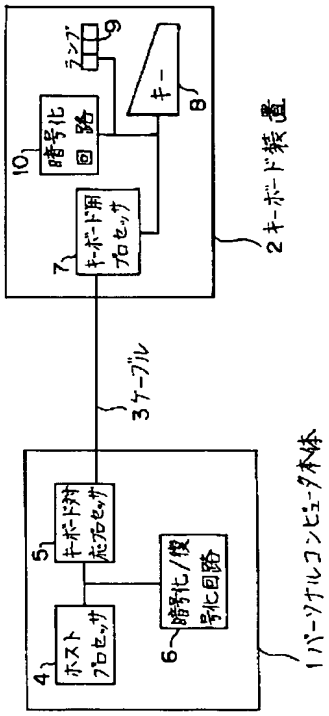
【図７】従来のキーボード装置及びパーソナルコンピュータ本体の構成の一例を示す図である。

【符号の説明】

１、６１　　パーソナルコンピュータ本体
２、６２　　キーボード装置
３、６６　　ケーブル
４　　ホストプロセッサ
５　　キーボード対応プロセッサ
６　　暗号化／復号化回路
７　　キーボード用プロセッサ
８　　キー
９　　ランプ
１０　　暗号化回路
６５　　光ケーブル
６３、６４　　光送受信機

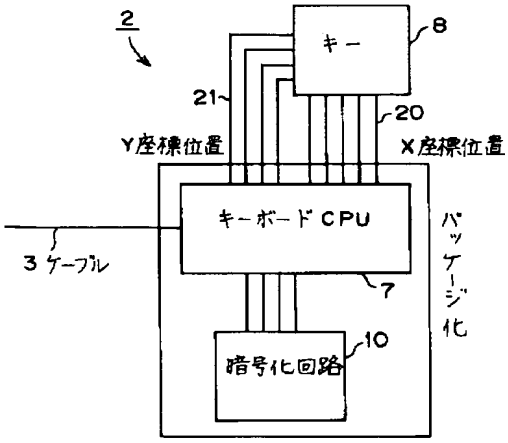
【図１】

本発明のキーボード装置の第1の実施形態の構成を示す図



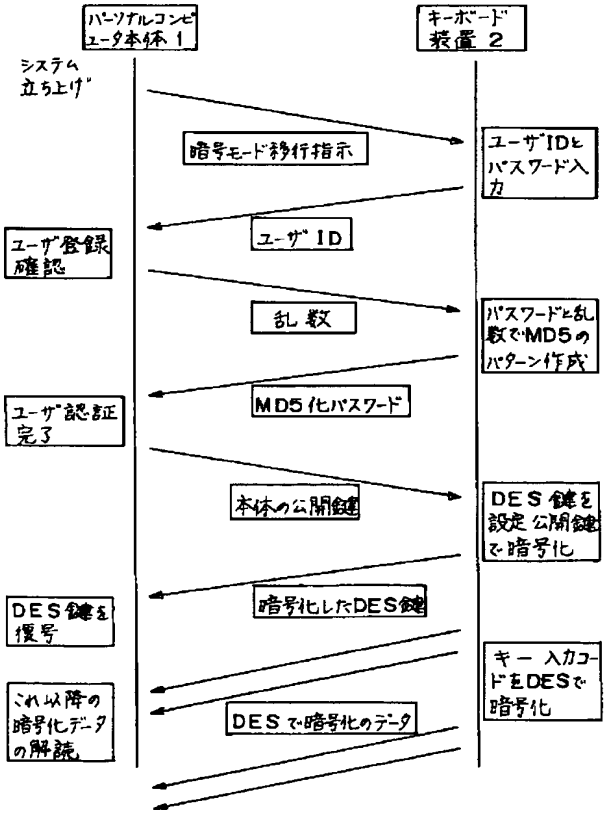
【図２】

本実施形態のキーボード装置の構成の一例を示す図



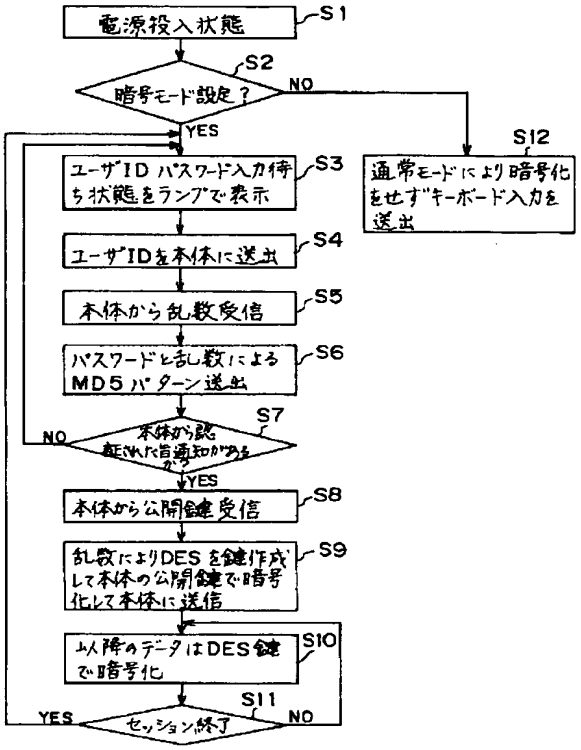
【図３】

本実施形態の一連の処理フローを表すタイムチャート



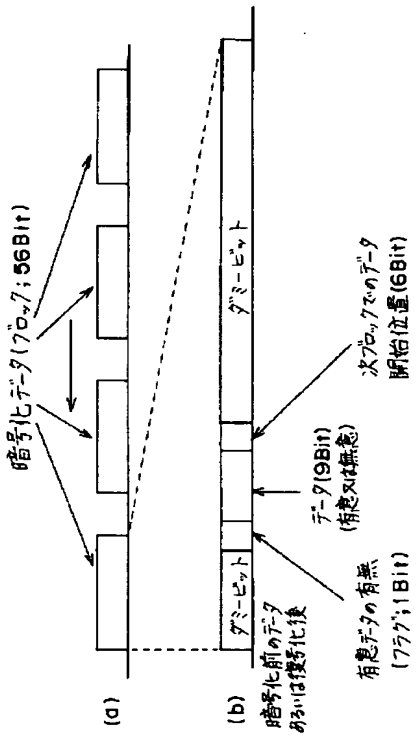
【図４】

キーボード装置側の一連の処理を示した図



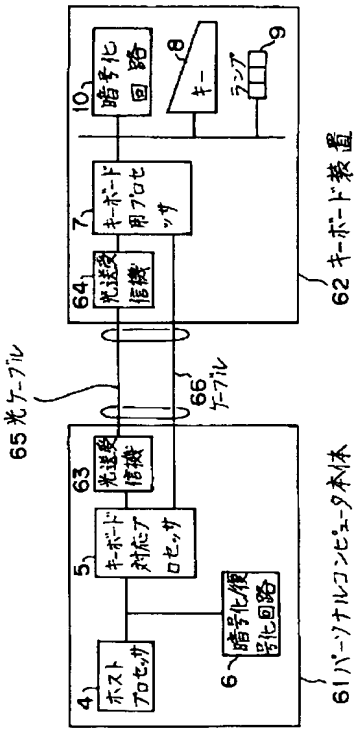
【図５】

本実施形態でキーボード装置からパーソナルコンピュータ本体に送信されるデータの構成を説明する図



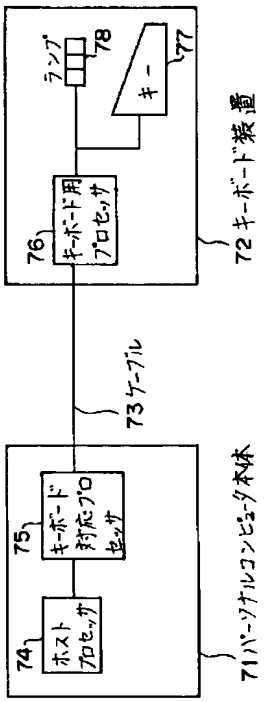
【図６】

本発明のキーボード装置の第2の実施形態の構成図



【図７】

従来のキーボード装置及びパーソナルコンピュータ本体の構成の一例を示す図



フロントページの続き

(51) Int.Cl.[6]	識別記号	FI	
H04L 9/36		H04L 9/00	673C
			673A
			685